AO 106 (Rev. 04/10) Application for a Search Warrant

FILED
JUL 13 2021
U.S. DISTRICT COURT-WVND
WHEELING, WV 26003

UNITED STATES DISTRICT COURT

for the

Northern District of West Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The residence located at
9909 National Rd., Valley Grove, WV 26060, and the person of Conner David Patterson

Case No. 5:21-MJ-49

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See "Attachment A-1" and "Attachment A-2"

located in the Northern District of West Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	Possession and Distribution of Child Pornography
18 U.S.C. § 2252A	

The application is based on these facts:

See Attached "Affidavit in Support of an Application for Search Warrant"

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

William Castilow, FBI TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: 7-13-21

Judge's signature

City and state: Wheeling, WV

James P. Mazzone, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF **9909 National Road, Valley Grove, West Virginia 26060, and the person of Conner David Patterson**	Case No. 5:21-MJ-49 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

I, William P. Castilow, a deputized Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) (hereinafter Affiant), being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 9909 National Road, Valley Grove, West Virginia, hereinafter "PREMISES", further described in Attachment A-1, for the things described in Attachment B. I further seek authorization to search the person of Conner Patterson, further described in Attachment A-2.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) assigned to the FBI Pittsburgh Division's Wheeling, West Virginia, Resident Agency (RA) in the Northern District of West Virginia (NDWV), where I work as a part of the West Virginia Child Exploitation and Human Trafficking Task Force. I have been employed with the Wheeling Police Department since February 2015. I presently am assigned to the Wheeling Police Department Investigations Unit to investigate a variety of criminal activity, including the investigation of violent crimes and major offenses such as fraud, violent crimes against children, and other violent criminal matters within the area of responsibility of the Wheeling Police Department.

3. During my training at the West Virginia State Police Department, Charleston, West Virginia, as well as on the job experience, I have received training in a variety of investigative and

legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause.

4. As part of my duties, I investigate criminal violations related to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code (U.S.C.) § 2252 and § 2252A. As part of my official duties in these matters, I have been exposed to examples of child pornography as defined in Title 18 U.S.C. § 2256.

5. The facts set forth below are based upon your Affiant's personal observations, reports and information provided to your Affiant by other law enforcement officials and obtained records. This Affidavit is intended to show that there is probable cause for this search warrant and does not purport to set forth all of your Affiant's knowledge of our investigation into this matter. I have set forth only the facts I believe are necessary to establish probable cause that evidence of violations of Title 18, U.S.C. § 2252 and § 2252A is located in the residence at **9909 National Road, Valley Grove, West Virginia, and on the person of Conner Patterson** (Attachments A-1 and A-2). The purpose of this application is to seize evidence of violations of Title 18, U.S.C. § 2252 and § 2252A, which among other things, make it a crime to possess, distribute, or receive, child pornography in interstate commerce by computer.

RELEVANT STATUTES

6. This investigation concerns alleged violations of Title 18, U.S.C. § 2252 and § 2252A, relating to material involving the sexual exploitation of minors.

7. Title 18, U.S.C. § 2252 and § 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them, as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using

any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (i.e., child pornography, as defined in 18 U.S.C. § 2256(8)).

CHARACTERISTICS OF PERSONS WHO TRAFFIC CHILD PORNOGRAPHY

8. As a result of the above-mentioned training and experience, your Affiant has learned that the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material includes, but is not be limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes, books, or similar items stored electronically on computers, digital devices or related digital storage media.

9. For the purpose of this Affidavit for search warrant, the following definitions apply to any/all references to minor, child, juvenile, sexually explicit conduct, person, knowledge, and child pornography.

a. Minor, child and juvenile means any person under the age of eighteen years.

b. Knowledge means knowing - or having reasonable cause to know, such as would warrant further inspection or inquiry.

c. Sexually explicit conduct includes any of the following, whether actually performed or simulated:

   i. Sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex;

   ii. Bestiality;

   iii. Masturbation;

   iv. Sadistic or masochistic abuse; or

   v. Lascivious exhibition of the genitals or pubic area of any person.

d. Child pornography means any visual depiction of a minor engaged in sexual explicit conduct. 18 U.S.C. § 2256(8)

10. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks. (Web sites, peer to peer file sharing networks, newsgroups, electronic bulletin boards, chat rooms, instant message conversations, e-mail, etc.)

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.

c. Trading with other persons with similar interests through shipments, deliveries and electronic transfer.

d. Producing and manufacturing these materials during actual contact with children.

11. These offenders collect materials depicting children engaged in sexually explicit conduct for many reasons. These reasons include, but are not limited to, the following:

a. For sexual arousal and sexual gratification.

b. These offenders use child pornographic materials the same way other people use adult pornography—to feed sexual fantasies.

c. Use as a means of reliving fantasies or actual encounters with the depicted children.

d. To lower children's inhibitions - A child who is reluctant to engage in sexual activity with an adult or pose for sexually explicit photographs can sometimes be convinced by viewing other children having "fun" participating in sexual activity. Additionally, peer pressure can have a tremendous effect on children. If other children are involved, the child might be led to believe that the activity is acceptable.

e. Use as blackmail - Children are often afraid that the illicit pictures and/or motion pictures taken of them will be shown to their friends or family. If the child threatens to tell his or her parents or the authorities, the existence of sexually explicit photographs/motion pictures is often an effective silencer.

f. As a commodity for exchange

i. Some offenders exchange illicit images or videos of children for other child pornographic images or videos.

ii. Some offenders send, cause to be sent, distribute, exchange, trade or sell these illicit materials to other people with similar interests as a means of gaining acceptance, status, trust and psychological support from these other persons.

iii. Some offenders exchange these illicit materials for means by which to contact other children (i.e. telephone numbers, e-mail addresses, screen names, etc.).

iv. The quality and theme of the material often determine its value as a commodity for exchange.

g. For profit.

i. Some offenders involved in the sale and distribution of child pornography are profiteers and are not sexually interested in children.

ii. Other offenders may begin nonprofit trading, which they pursue until they accumulate certain amounts or types of images, which they then sell to distributors for reproduction in commercial child-pornography magazines or made available on the Internet for downloading.

iii. Others offenders may combine their sexual interests in children with their profit motive. Thus an illicit image of a child taken by a local offender in any community in the United States can end up in a commercial child-pornography magazine or on the Internet with worldwide distribution.

12. These offenders view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Consequently, these offenders prefer not to be without their child pornographic material for any prolonged time period and often go to great lengths to conceal and protect their illicit collections from discovery, theft, or damage. To safeguard their illicit materials or digital devices which contain their illicit materials, these people may employ the following security measures:

a. The use of safes and safe deposit boxes.

b. The use of concealed compartments or concealed rooms within premises or other structures that they occupy or have control of.

c. The use of storage facilities outside their immediate residence (outbuildings, motor vehicles, animal cages, recreational vehicles, vessels etc.).

d. The use of Internet-based data storage services.

e. Rental of storage facilities.

f. Recording onto media that contains false, misleading or no title(s).

g. The application of digital security technologies, including, but not limited to, password protection, encryption and steganography.

13. These offenders may send, cause to be sent, distribute, exhibit, possesses, collect, display, transport, manufacture or produce materials depicting children fully clothed, in various stages of undress or totally nude, in various activities and not necessarily sexually explicit. These materials may include, but not be limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes, books, or similar items stored electronically on computers, digital devices or related digital storage media. This material is known as "child erotica." Although it may not meet the definition of child pornography, it is often probative of an offender's sexual interest in children and criminal intent.

a. These pictures may be cut out of printed media (magazines, newspapers, books, etc.), downloaded from the Internet or surreptitiously taken or recorded by the offender from afar.

14. In the case of materials which depict a child in the nude or posed in a sexually suggestive manner, there is a high probability that the child was molested before, during, or after the photo-taking and/or video session because the act of the posing is such a great sexual stimulus for the offender taking the pictures and/or making the videos.

a. These materials are used by these offenders as a means of establishing and sustaining fantasy relationships.

b. These photos and/or videos are rarely, if ever, disposed of and are revered with such devotion that they are often kept in close proximity to the offender and occasional upon the offender's person and such.

15. These offenders fear discovery and may maintain and operate their own photographic production and reproduction equipment. This may be as simple as the use of "instant" photo cameras, video equipment or as complex as a completely outfitted photographic studio or photograph development laboratory.

TECHNICAL TERMS

16. Based on my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers and child pornography:

a. Internet. The term "Internet" is defined as the worldwide network of computers — a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider, which operates a host computer with direct access to the Internet. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Internet Service Providers. Individuals and businesses obtain access to the Internet through internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data, and written record format.

c. Internet Protocol Addresses. An Internet Protocol ("IP") Address refers to a unique numeric or alphanumeric address used to connect to the Internet. IP Addresses can be "dynamic," meaning that the ISP assigns a different

unique number to a device every time it accesses the Internet, or "static," meaning an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet. There are two versions of IP addresses: IPv4 and IPv6. IPv4 is the most widely used IP, and uses four groups of numbers separated by periods in a 32-bit address scheme (e.g., 121.56.97.178). IPv6 uses colons to separate eight alphanumeric groups (e.g., 2001:0:1760:e3e7:1858:2cea:d075:6c4c). In a simple example, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is more typical is that one home may connect multiple digital devices to the internet simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home connect to the Internet via a router or hub. The devices connect to the router or hub, and the hub connects to the Internet. Internet activity from every device attached to the router or hub is using the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. Most ISPs maintain records of which subscriber was assigned to which IP Address during an online session.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

17. A significant aspect of the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. For example, users of BitTorrent, a type of P2P software, wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of

files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the "torrent" based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file.

18. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

19. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. A user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a BitTorrent user downloading an image file receives the entire image from one computer.

20. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers. No two identical IP addresses can operate on the same segment of the Internet simultaneously.

PROBABLE CAUSE

21. On March 8, 2021, your Affiant and Detective Adams, who is also a Wheeling Police Department Detective assigned to the FBI's West Virginia Child Exploitation and Human Trafficking Task Force as a TFO, were assigned National Center for Missing and Exploited Children (NCMEC) CyberTipline Report #85523352, in which Facebook identified a possible video, MD5 # aaa1b0f0d5b0131fa2707d69046026c3, depicting child pornography, and submitted the file to NCEMEC. The report provided suspect information as [redacted].

22. The IP addresses from which the file was sent, 2601:54a:302:ded0:d9a3:ca20:441c:55da, was associated with an unknown physical location in or near Wheeling, WV. The recipient IP address was associated with an unknown physical address in or near Valley Grove WV.

23. Investigators viewed the video, which showed two unknown prepubescent juvenile males were engaging various sexual acts, including oral and what appeared to be anal sex.

24. On March 9, 2021, I obtained an administrative subpoena for Comcast Communications for IP address 2601:54a:302:ded0:d9a3:ca20:441c:55da.

25. On March 18, 2021, at approximately 1318 hours, I received the IP address results from Comcast. The report provided a subscriber name of [redacted], Wheeling WV 26003. I ran [redacted]'s WV driver's license, which returned to [redacted] Wheeling, Ohio County WV 26003. On 03-19-2021 I obtained a State search warrant for [redacted].

26. On March 20, 2021 myself, Det. Adams, and Ofc. Hoehn, who is a Wheeling Police Department Patrol Officer, proceeded to [redacted] to execute the State search warrant. Upon arrival, I made contact with [redacted] and advised her we had a search warrant. We

proceeded inside and made contact with [redacted] who was asleep in the room. We placed [redacted] and Zachary in the living room and secured the residence.

27. Det. Adams escorted [redacted] back to his room to speak with him. [redacted] stated he had child pornography on his cell phone and that he sent the video of the prepubescent juvenile males to a person named [redacted]. After [redacted] spoke with Det. Adam, we began a search of his room. We took custody of [redacted]'s Iphone and a LG smartphone, which was placed on the shelves next to his bed.

28. Once at Headquarters, Detectives began to examine [redacted]'s cell phone. In the photos application I observed multiple nude images and videos of prepubescent juvenile males performing sexual acts and exposing their penis.

29. I then accessed [redacted]'s Snapchat and located a text thread between him and user name [redacted]. In the text thread, I located a photo of a young prepubescent juvenile male who appears to be performing oral sex. Above the photo is what appears to be a prepubescent juvenile male exposing his anus and penis.

30. On March 26, 2021, I received a return from Facebook in response to a State search warrant on the account of [redacted], which I previously served to Facebook on March 9, 2021. I located the MD5 file which referenced above. It was sent to [redacted]. There was no other child pornography located. I located a thread between a person named Conner Patterson and [redacted] on February 6, 2021. It's important to note Conner Patterson is consistent with the Snapchat profile of [redacted].

31. On March 22, 2021, I obtained a State search warrant for Snapchat user [redacted], which was served through Snapchat's law enforcement portal.

32. On May 10, 2021, I received the search warrant results from Snapchat. The subscriber information provided in the return listed the username as [redacted], the user e-mail as [redacted], and the display name as *Conner*. Upon review, I located multiple photos and videos of child pornography. I also located IP address 71.61.24.39, which indicated the Snapchat profile [redacted] was logged in and logged out on March 21, 2021.

33. I searched the IP address, which returned to Comcast Communications. I obtained an administrative subpoena and served it to Comcast through their Law Enforcement Portal.

34. On June 2, 2021, I received notification form Comcast providing [redacted] as the subscriber and the listed address of 9909 National Road, Valley Grove, WV 26060. It appears [redacted] is the mother or a family member of Conner David Patterson.

35. On June 3, 2021, I located Conner David Patterson's driver's license which lists 9909 National Road, Valley Grove, WV 26060 as his address.

36. Your Affiant has learned through investigation that Patterson lives in 9909 National Road, Valley Grove, WV 26060. Patterson's WV driver's license returns to 9909 National Road as well as the IP address associated with his Snapchat account. A search of Conner Patterson through TLO also returns the address of 9909 national Road, Valley Grove, WV 26060.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

39. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

40. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

41. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

42. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

43. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates on which files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-

virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the

computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

44. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu

of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

46. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

47. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks,

and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000

double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500-gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

48. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregated from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point

toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment and can require substantial time.

49. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregated from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and can require substantial time.

50. Digital device users can attempt to conceal data within digital devices through several methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence,

contraband, or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

51. I know that when an individual uses a digital device to distribute or attempt to distribute child pornography, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. As discussed herein, based on my training, and experience I believe that digital devices will be found during the search. As previously discussed, the target of the investigation may have used Peer-to-peer file sharing as a method of transferring digital files. I know that Peer-to-peer file sharing is predominantly used on computers but may also be used via mobile devices.

53. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device

through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user

of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

i. The proposed warrant does not authorize law enforcement to compel PATTERSON to state or otherwise provide the password or any other means that may be used to unlock or access the device(s).

CONCLUSION

54. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A-1, and the person described in Attachment A-2, to seize the items described in Attachment B.

55. I further request that the Court seal the warrant and the affidavit and application in support thereof, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office and may be served on Special Agents and other investigative and law enforcement officers, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, as necessary to effectuate the warrant. These documents pertain to and discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation. Sealing these documents will also better ensure the safety of agents and others.

Respectfully submitted,

William P. Castilow
Wheeling Police Department
FBI Task Force Officer
West Virginia Child Exploitation and
Human Trafficking Task Force

Subscribed and sworn to before me on July 13, 2021.

UNITED STATES MAGISTRATE JUDGE
JAMES P. MAZZONE

ATTACHMENT A-1

Property to be Searched

1. The premises to be searched is **9909 National Road, Valley Grove, WV 26060**, a blue/grey single-story house with a basement garage.
2. The premises to be searched shall also include any and all yards, outbuildings, storage areas, motor vehicles, recreational vehicles, motor homes, vessels, garages, carports, sheds, animal cages or houses and mailboxes assigned, located at or part of the premises described in the first paragraph of this section.

ATTACHMENT A-2

Person To Be Searched

The person of **CONNER DAVID PATTERSON** is described as a white male 5'-05'' 150 lbs, blue eyes, black hair, DOB: [redacted]2000, social security number ending in 7981.

ATTACHMENT B

Property to be seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § § 2251, 2252 and 2252A.

1. Computers or storage media used as a means to commit the violations described above, including any computer, computer hard drive, computer system and related peripherals; such as external hard drives, flash drives, thumb drives, magnetic media floppy disks, optical disks, computer floppy disks, digital cameras, tapes, cassettes, cartridges, and any electronic data storage devices including, but not limited to, CD-Roms, DVDs, cellular telephones which have the capability to store images, gaming systems (Xbox, Playstation, Nintendo, etc.), and other storage mediums such as Apple's IPOD line of products and Microsoft's Zune digital players.
2. Any passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

6. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

7. Any evidence involving online or cloud storage; online or cloud storage accounts; downloads or transmissions to an online or cloud storage account; online or cloud storage software.

8. Any evidence related to the use of BitTorrent software.

9. Any property including digital devices on the person of Conner David Patterson, including but not limited to, any pockets in his clothing, and any bags or other containers carried or held by him, provided that he is located within the Northern District of West Virginia at the time of the search.

During the execution of the search of the Subject Premises and person described in Attachments A-1 and A-2, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.